UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,179	12/02/2003	Simon Robert Walmsley	PEA16US	5306

24011 7590 07/26/2010
SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
07/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

pair@silverbrookresearch.com
patentdept@silverbrookresearch.com
uscorro@silverbrookresearch.com

Office Action Summary	**Application No.** 10/727,179	**Applicant(s)** WALMSLEY ET AL.	
	Examiner DANIEL L. HOANG	**Art Unit** 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

While examiner does not necessarily agree with the arguments presented by applicant in the most recent correspondence, for the sake of prosecution, a new grounds of rejection is set forth below.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3, 5-8, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hameau et al., US PGP No. 20020107798. and further in view of Auerbach, US Patent No. 5673316

As per claim 1:

Hameau teaches:

An integrated circuit comprising

a processor and non-volatile memory,

[see paragraph 50, "CPU" and paragraph 46, "ROM"]

the non-volatile memory storing a first number and a second number,

[see paragraph 50, wherein the sixteen byte random number NaC is viewed as the "first random number"]

[see paragraph 58, wherein the secret session key Ks is viewed as the "second random number"]

wherein the second number is the result of an encryption function taking the first number and secret information as operands,

[see paragraph 58, wherein the session key Ks is the result of the random number NaC and the secret master key Km. The secret master key Km is viewed as the "secret information".]

~~the secret information not being stored by the non-volatile memory,~~

~~*[see paragraph 65, wherein "the intermediary results are stored in registers or in RAM" not stored in the ROM]*~~

the first number being a random number; and

[see paragraph 50, "sixteen byte random number"]

the integrated circuit comprising software configured to decrypt the second number using the first number, thereby to determine the secret information as required.

[see paragraphs 72 and 73, wherein the session key is derived]

The Hameau reference has been discussed above. Hameau is mute in teaching that the secret information is not stored by the non-volatile memory. For this limitation, examiner relies on the Auerbach reference. Auerbach teaches at col. 1, lines 54-67 and col. 2, lines 1-40 of part encryption keys (PEKs) which are not stored by the user seeking to decrypt encrypted information. Auerbach teaches that maintaining a key database at a server instead of at the distribution and/or client allows the system to maintain a cleaner separation of trust between the document server and the buy server. it would have been obvious to one of ordinary skill in the art to modify the Hameau reference to include the *separation of trust component taught by Auerbach in order to create an environment where there exists a measure of trust between server and client (see Auerbach background).*

As per claim 3, Hameau teaches:

An integrated circuit according to claim 1, wherein the first and second numbers are of the same length.

> *[see paragraph 23] "storage means of said microchip storing a <u>symmetric secret encryption key</u> and an asymmetric public key and said security device storing the <u>same symmetric secret encryption key</u>." Both are the same and thus clearly are the same length.]*

As per claim 5, Hameau teaches:

An integrated circuit according to claim 1, wherein the encryption function is an XOR logical function.

> *[see paragraph 63] "The part K.sub.S1 is re-injected through a first input of a logic circuit of the "exclusive-OR" type, referenced XOR."*

As per claim 6, Hameau teaches:

An integrated circuit according to claim 5, wherein the software is configured to decrypt the second number by performing an XOR logical function using the first and second numbers as operands.

> *[see paragraph 65] "the "exclusive-OR" logic operation can be performed by means of software instead of using a specific logic circuit XOR, by calling a routine stored in "ROM" memory 1, for example, under the control of the microprocessor CPU."*

As per claim 7, Hameau teaches:

A method of manufacturing a plurality of integrated circuits in accordance with claim 1, including the steps, for each integrated circuit, of: determining the first number, and the secret information; generating the second number by way of an encryption function that uses the first number and the secret information as operands; storing the first and second numbers on the integrated circuit.

> *[see paragraph 80] "The method makes it possible to load, into each smart card CP, its own key, or in other words a different key than the other smart cards.*

As per claim 8, Hameau teaches:

A method according to claim 7, wherein the first number is different amongst at least a plurality of the integrated circuits.

[see paragraph 80]

As per claim 10, Hameau teaches:

A method according to claim 7, wherein the first number is stored on the integrated circuit first, then extracted therefrom for use in generating the third and thence the second number.

[see rejection of claim 1, wherein the master key is stored on the smart card and then used to derive the remaining security data]

Claims 4 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hameau and Auerbach as applied to claim 1 above, and further in view of Pires (US Patent No. 6,269,164.

As per claim 4:

An integrated number according to claim 1, wherein the first number is a random number that was generated using a stochastic process.

The Hameau reference has been discussed above. Hameau does not expressly disclose that the first number is a random number that is generated using a stochastic process. Pres teaches of a stochastic key.

[see col. 18, lines 2-7] "stochastic key scrambling method previously described is particularly well suited to the creation of good keys. As stated before, a good key is one made by a process that distributes the keys it generates evenly over the entirety of the available key space regardless of the input used to create it."

It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the Hameau reference to incorporate the teachings of Pires in order to *include usage of a random key generated using a stochastic process in order to improve upon the security of the key and to generate a key that is difficult to obtain because it is created through a random process.*

As per claim 9, Hameau teaches:

A method according to claim 8, wherein the first numbers are determined randomly, pseudo-randomly, or arbitrarily.

[see rejection of claim4 wherein a stochastic process leads to randomness]

---

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2436

/David García Cervetti/

Primary Examiner, Art Unit 2436